NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RFID MEETS GWOT: CONSIDERING A NEW TECHNOLOGY FOR A NEW KIND OF WAR

by

Kevin Lee Kirby

June 2006

Thesis Advisor:	Michael Freeman
Second Reader:	Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE RFID Meets GWOT: Considering a New Technology for a New Kind of War	5. FUNDING NUMBERS
6. AUTHOR(S) Kevin Lee Kirby	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to provide insight into the potential benefits that Radio Frequency Identification (RFID) technology may provide USSOCOM and other commands in the Global War on Terror. This thesis will explain the basic concept behind RFID, and cite some of the current day applications of today that are revolutionizing the civilian sector. More importantly, this thesis will introduce conceptual security applications that could benefit USSOCOM today, highlighting the possible successes and downfalls that these applications might include.

14. SUBJECT TERMS Radio Frequency Identification, Security Applications, Insurgency, Counterinsurgency	15. NUMBER OF PAGES 71
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RFID MEETS GWOT: CONSIDERING A NEW TECHNOLOGY FOR A NEW KIND OF WAR

Kevin Lee Kirby
Major, United States Army
B.S., Radford University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
June 2006

Author: Kevin L. Kirby

Approved by: Michael Freeman
Thesis Advisor

Dorothy Denning
Second Reader

Dr. Gordon H. McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to provide insight into the potential benefits that Radio Frequency Identification (RFID) technology may provide USSOCOM and other commands in the Global War on Terror. This thesis will explain the basic concept behind RFID, and cite some of the current day applications of today that are revolutionizing the civilian sector. More importantly, this thesis will introduce conceptual security applications that could benefit USSOCOM today, highlighting the possible successes and downfalls that these applications might include.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the following individuals for their assistance in making this thesis possible. First I would like to thank Professors Michael Freeman and Dorothy Denning for offering to advise me throughout this process. I would also like to thank Professor Richard Bergin for describing in great detail the capabilities of radio frequency identification technology (RFID). Lastly, I must thank Adrian Hawley of Hills Numberplates Ltd. for providing me with extensive information regarding their RFID products.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Since the terrorist acts of 9/11 the United States has had to make many adjustments in order to improve the security of the nation and its interests abroad. Within days of the attacks, the United States responded to the terrorist network responsible for those attacks by initiating the Global War on Terror (GWOT). At first there were many successes in both Afghanistan and Iraq, but as the passing of time has shown, what seemed to be a relatively easy objective has evolved into a complex endurance event. Some experts agree that the solution will most likely involve massive and lengthy efforts at addressing the underlying causes of this global insurgency. With no relief in sight, some citizens of the United States have grown weary of their government's efforts and are concerned over the growing number of U.S. casualties. The potential length of the GWOT, coupled with the cost in terms of money and human life places considerable pressure on the Department of Defense of the United States to end the war in Iraq.

In April of 2006, six former generals from the United States armed forces began to openly criticize the Secretary of Defense, Donald Rumsfeld, for the difficulties the armed forces faced in Iraq. One of the critics, retired Marine Lieutenant General Gregory Newbold, formerly the Pentagon's top operations officer, was quoted in Time magazine as saying, "We need fresh ideas and fresh faces. That means, as a first step, replacing Rumsfeld and many others

unwilling to fundamentally change their approach."[1] While this thesis in no way addresses the performance of any leaders in the United States government, it does deal with Lieutenant General Newbold's suggestion of fresh ideas and a fundamental change in approach.

While it is possible that some aspects of the GWOT could take decades to change, a greater sense of security is needed now in order to establish the foundation toward a better future in places like Iraq and Afghanistan. Throughout history it has been necessary for some leaders and governments to impose a relatively extreme form of social control to keep order and effectively govern the people. In today's GWOT, the United States does not have the required manpower to maintain accountability over the populations in countries in which we are currently involved, but perhaps by using technology which is already available, the United States can gain the upper hand against the terror network.

A. PURPOSE

This thesis provides insight into the potential benefits that Radio Frequency Identification (RFID) technology may provide USSOCOM in the Global War on Terror. Secondly, this thesis provides a basic background of RFID technology and explains some of its current applications today. Finally, this thesis recommends two applications of RFID technology that can benefit the U.S. efforts in the GWOT, and discusses their advantages and disadvantages.

Chapter II of this thesis provides a basic understanding of what RFID is, key terminology, and how it

[1] Reuters, "U.S. Retired Generals Debate over Rumsfeld," MSNBC 16 April 2006 [website]; available from http://www.msnbc.msn.com/default.aspx?id=9974867; accessed 21 April 2006.

works. Chapter III will explain some of the current applications of RFID today. Chapter IV explains two applications for RFID technology, which could help the governing body gain the advantage over its adversaries. Chapter V covers the potential advantages and disadvantages of implementing these RFID concepts, and Chapter VI provides a summary of the thesis.

B. RELEVANCY

As of 1 June 2006 there were 2,764 members of the United States Armed Forces listed as killed in Afghanistan and Iraq.[2] This growing number has caused much debate in the United States' political realm and has also triggered military leaders to ask how they can lessen the loss of American lives. For example, the Improvised Explosive Device (IED) accounts for more then 32 percent of US fatalities in Iraq. These high figures have solicited a great response from some organizations, including the Naval Postgraduate School in Monterey, California, which has created an entire graduate level seminar dedicated to producing countermeasures to combat the lethality of IEDs. Similar to IEDs, vehicle-related deaths caused by hostile intentions are one of the leading causes of fatalities amongst members of the U.S. Armed Forces in Iraq.[3] Without question it is to the benefit of the Department of Defense to explore every possible solution in reducing U.S. fatalities in war torn areas.

---

[2] Department of Defense, Daily Casualty Report, 1 June 2006 [website]; available from http://www.defenselink.mil/news/casualty.pdf; Internet; accessed 1 June 2006.

[3] Michael White, "Iraq Coalition Casualty Count," *Icasualties*, 1 June 2006 [homepage]; available from http://www.icasualties.org/oif/default.aspx; Internet; accessed on 1 June 2006.

As demonstrated by the Malayans and British in Malay during the 1950s, providing security to the people is essential in defeating the insurgency.[4] With this principle in mind, it should be the intent of the government to gain as much information about the insurgents as possible, in order to reduce Iraqi and U.S. fatalities. Nathan Leites and Charles Wolf, insurgency experts formerly employed at The Rand Corporation, suggest that "efficient action requires information." Additionally, Leites and Wolf point out those members of an insurgency have greater potential to gather information than the government they oppose. Leites and Wolf explain that the government has a greater challenge in collecting information on the insurgents, because the insurgent must "play it safe." The insurgents must remain "small, invisible, tightly organized, highly security-conscious, and hard to penetrate" in order to ensure their survival. As a result, gaining information on these organizations is a great challenge for governments. On the other hand, insurgents often have an advantage in collecting information on the authorities, because they are "large, visible, usually loosely organized, and easy to penetrate."[5] It is this void of information that can perhaps be filled by using RFID technology. In turn, this could result in greater security and possibly change the direction of the counter-insurgency mission in Iraq.

---

[4] Frank Pelli, "Insurgency, Counterinsurgency, and the Marines in Vietnam," Global Security, 1990 [report online]; available from http://www.globalsecurity.org/military/library/report/1990/PFD.htm; Internet; accessed 8 June 2006.

[5] Nathan Leites and Charles Wolf, *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts*, (Chicago: Markham Publishing Company, 1970), 132.

C. REFERENCES AND DEFINITIONS

First, it is important to understand that even though there are many references to Operation Iraqi Freedom throughout this thesis, by no means are the concepts that are recommended within exclusive to that country. However, to date, Iraq is the dominant area of operations for the United States Armed Forces and the greatest source of U.S. fatalities in terms of the GWOT. Therefore, Iraq is a prime example for this thesis, but the recommendations within are designed to be applicable in any unstable country. Additionally, with Iraq being one of the primary fronts in the GWOT, it has received much attention from the media, which inherently includes a greater number of reports, more statistics, and general analysis than other countries involved in the GWOT. Consequently, this provides more supporting information for the thesis.

The "Global War on Terror" is an ambiguous phrase, because by definition, we are not truly facing terrorists. The opponent the United States and its allies confront today may be better understood as a network of organizations involved in a global insurgency. While the enemy may use tactics of terror, they are still insurgents and therefore they will be labeled as such throughout this thesis.

Lastly this thesis will often refer to specific configurations of RFID tags, RFID readers, and databases as "RFID technology". This has been done to simplify the reading, but it should be noted that this term is only referencing the specific configurations mentioned in chapter IV and not RFID in a broader sense.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WHAT IS RFID

A. THE ORIGINS OF RFID

Radio Frequency Identification (RFID) is currently being used in various applications all around the world. An average citizen in the United States may come in contact with RFID technology a few times a day, and in most cases it will be transparent to them. The frequency in which RFID is being used is growing at a rapid rate, and in time, will most likely impact most people's lives. While RFID may increase efficiency and provide benefits to businesses, it will probably remain unnoticed to most consumers. Nevertheless, it is important to understand the technology that is being used. The main intent of this chapter is to provide an understanding of the origins of RFID and a basic overview of how RFID works.

> Radio Frequency Identification (RFID) technology is an automatic way to collect asset data (identification, location, transaction, time) quickly and easily without human intervention or error.[6]

There are very few definitions for RFID listed in today's dictionaries, such as the one quoted above. Logically, one may assume that RFID has not yet hit the mainstream dictionaries, such as Webster, because it is such a new technology. However, this is not the case; RFID tags with rewritable memory were first given a patent in the United States in 1973. It was also in the 1970s that that the U.S. Department of Energy asked the Los Alamos National Laboratory to develop a method which would help

[6] "Introduction to RFID," Identec Solutions, [homepage]; Available from http://www.identecsolutions.com/ intro_to_rfid.asp; Internet; accessed 3 May 2006.

keep track of the nuclear material within the United States. Using radio frequency, the scientist working at the laboratory placed a transponder in the trucks carrying the nuclear material. When it approached an entrance or exit at a secure facility, a corresponding reader would detect the signal and provide the identification of the shipment, and perhaps other additional information, such as the identity of the driver.[7]

While RFID technology existed in the 1970s, the roots of RFID trace back to World War II. The discovery of radar played a large role in the war and lent to the basic concepts of RFID.[8] Radar provided a great advantage to both sides in the war by giving advance warning to those on the ground of an approaching aircraft. However, the one significant disadvantage that radar suffered from was its inability to distinguish the identity of the aircraft, friend or foe. In response to this weakness, the Germans discovered that if the aircraft were to change its flight orientation, then it would register differently on the radar signal by reflecting a more unique signature. As a consequence, the German pilots made it their standard operating procedure to execute a roll on their approach back into their home base, thus providing the German radar operators with an identifiable signature. While there was no transponder on the planes themselves, the Germans manipulated the aircrafts orientation in order to reflect a different signal back to the radar, essentially

[7] "The History of RFID Technology," RFID Journal [journal online]; available from http://www.rfidjournal.com/article/articleview/1338/1/129; Internet; accessed 21 April 2006.

[8] Jeremy Landt, Shrouds of Time: The History of RFID, AIM [whitepaper online]; available from http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf; Internet; accessed 26 April 2006.

transforming the entire aircraft into a transponder. This application is recognized by some as the first passive RFID system.[9]

B. HOW DOES RFID WORK

Before understanding how an RFID system works, it is helpful to first become familiar with the components. There are two main components of an RFID system: the tag and the reader.

1. The Tag

A radio frequency identification tag "is a device that can store and transmit data to a reader in a contactless manner using radio waves."[10] Tags are the foundation of a RFID system, without them the other components would have no function. RFID tags are also commonly referred to as transponders within the RFID community, and to further complicate things, there are many different forms that the devices come in such as smart labels, simple tags, or smart cards.[11] However, to keep things simple, this document will refer to them only as tags. The tag itself is the component which is affixed to the object that is to be identified, such as the RFID chips placed under the skin of animals for identification purposes. Perhaps the largest distinguishing factor from one tag to the next is whether or not it is a passive or active tag.

---

[9] "The History of RFID Technology," 1.

[10] Sandip Lahiri, *RFID Sourcebook*. (Upper Saddle River: IBM Press, 2006), 9.

[11] "Glossary of RFID Terms," RFID Journal [journal online]; available from http://www.rfidjournal.com /article/articleview/1338/1/129; Internet; accessed 21 April 2006.

Figure 1. Various passive tags. (From: RFID Sourcebook, p. 13)

The passive tag, unlike the active tag, does not have its own power source, such as a battery. Passive tags, as the name implies, are passive in the sense that they do not transmit any information regarding their identity until they are prompted to. Even once they are prompted by a reader to wake up, the passive tag does not transmit its own signal; instead it reflects the signal that the reader sent initially, thus returning a unique identity. Not needing to power its own signal, passive tags require less subcomponents and have no moving parts. Therefore, passive tags tend to be smaller than active tags. While the smaller size may offer some advantages, this may come at the expense of the tag's capabilities. Typically, the range for a passive tag is between 1 inch and 30 feet.[12] Generally speaking, passive tags are less expensive than active tags and vary in price from 20 cents to several dollars. Tag prices may reflect many different factors. The first factor is the frequency at which the tag responds; high-frequency tags, for example, require more copper in the antenna, thus raising the price. The amount

[12] Lahiri, 9.

of memory a chip offers, the packaging around the tag, and the quantity ordered are a few other factors that can affect the price of a passive tag.[13]

Figure 2. An active RFID tag. (From: RFID Sourcebook, p. 18)

Active tags are different in that all of them have their own power supply. This is what enables an active tag to transmit its own signal and not have to rely on the reader. While this does offer more capabilities to the tag, it also increases its size. One of the most significant increases in capabilities is the range from which a reader can detect the tags signal; some tags can be read from 300 feet away.[13] Additionally, the microchips in active tags are typically larger and offer greater capabilities than those in passive tags. Of course, greater capability comes at a greater price; active tags typically range from $10 to $50 a piece. Cost factors include the size of the battery, the memory in the microchip, and the packaging around the tag.

[13] "RFID System Components and Costs," RFID Journal [journal online]; available from http://www.rfidjournal.com /article/articleview/ 1338/1/129; Internet; accessed 21 April 2006.

2. The Reader

A RFID reader, also known as an interrogator, is described by one expert as "a device that can read from and write data to compatible RFID tags."[14] Readers, like tags, come in two variations, stationary and handheld, both of which offer different capabilities at different prices.

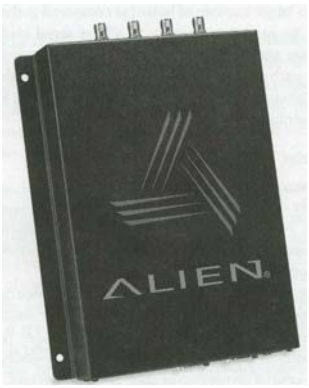

Figure 3. A fixed RFID reader. (From: RFID Sourcebook, p. 26)

Stationary readers, commonly referred to as fixed readers, are permanently affixed readers. These may be placed on portals, walls, street lights, or any other suitable object; however, these readers are not confined to static objects. For example, a stationary reader may be mounted onto a police car, as suggested later in chapter IV, and still engage with signals as they pass by tags within range. Stationary readers are generally less expensive than handheld readers and are more prevalent in the industry today.[15]

[14] Lahiri, 22.

[15] Ibid., 26.

Figure 4. A handheld RFID reader. (From: RFID Sourcebook, p. 30)

Handheld readers are sometimes referred to as mobile readers. However, one key difference is that a mobile reader may not require a person to hold it and may simply be attached to a mobile object; whereas handheld models are, as the name implies, held by an operator. While handheld readers may not be able to offer as competitive a price as a stationary reader, they offer mobility and perhaps more potential applications. Depending on the functions they perform, handheld readers may range from $500 to $3,000.[16] Unlike stationary readers, handheld readers do require manning, but it usually only requires one person to operate.

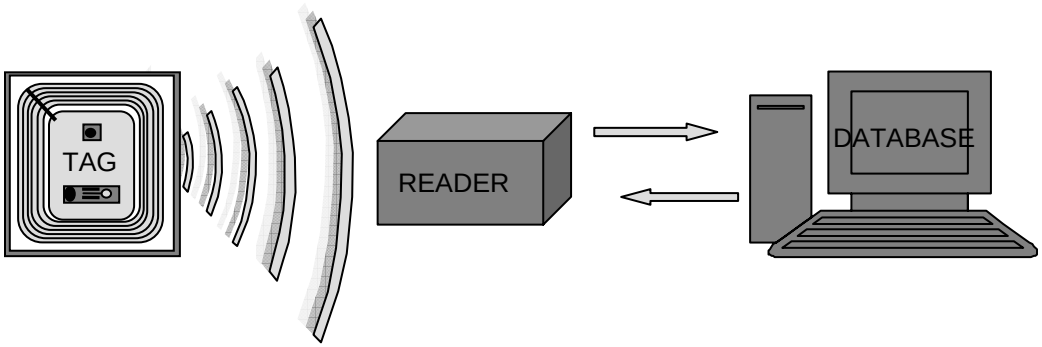

Figure 5. An example of an RFID system working together.

[16] "RFID System Components and Costs," 1.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RFID TODAY

To understand the potential of radio frequency identification technology in the future, we need to look no further than the applications of today. Two of the early major uses of RFID included garage door openers and animal identification, but today's uses have expanded into many different areas, such as automatic toll collection, access control, security, equipment tracking and payment, amongst others.[17] In this chapter we will examine some of the current applications of RFID today and some of which are to debut in the very near future.

A. LOGISTICS

In June of 2003, Wal-Mart announced a mandate that would require its top 100 suppliers to equip their shipments of merchandise with RFID technology by 2005. Wal-Mart is requiring that the suppliers use RFID tags on the pallets and individual cases that they ship to the Wal-Mart distribution center. This will enable the distribution center to instantaneously keep an accurate inventory of any tagged item that either enters or exits the warehouse. Ideally, as each Wal-Mart store is being equipped with the same readers, they too will have the ability to instantly inventory items that are arriving, as well as those that are in the store's warehouse or on the sales floor. The benefits of having a full understanding of the stock that is available at any given time will pay great dividends. Since Wal-Mart first introduced this mandate, they have broadened their RFID initiative to include the next 200 biggest suppliers and they have

[17] Simson Garfinkel and Beth Rosenberg, eds. RFID: Applications, Security, and Privacy (Upper Saddle River: Addison Wesley, 2006), 6.

equipped more than 600 of their Wal-Mart locations with RFID readers. Conveniently, Wal-Mart is in a position of power and has not had to pay for the burdens that have been placed upon its suppliers. It was determined that the first 137 suppliers that agreed to comply with the mandate spent an average of $500,000 to institute the RFID mandate within their businesses. While start up cost has proven to be significant, the end results of savings may reach into the billions annually. According to a report by A.T. Kearney, these RFID applications could reduce labor costs by 7.5 percent and increase labor efficiency by ten to twenty percent. Additionally, "a mere one percent reduction in out-of-stock would translate to $2.5 billion in added annual sales, since Wal-Mart's total annual sales are about $250 billion."[18]

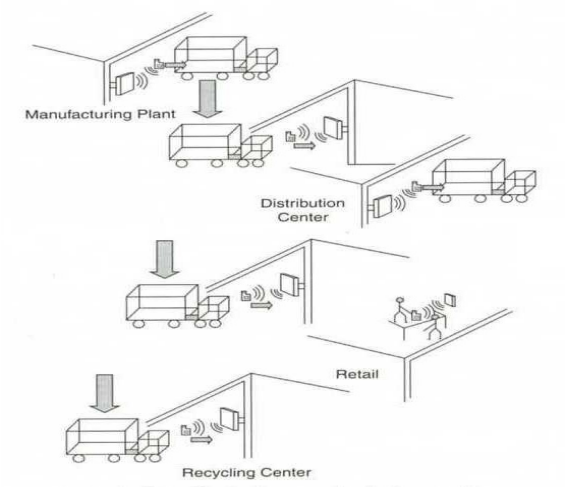

Figure 6. An example of RFID in supply-chain operations. (From: RFID Sourcebook, p. 67)

While Wal-Mart might have been the first large business to mandate the implementation of RFID technology into its logistics management, it is definitely not alone.

[18] Robert Kleist and others, RFID Labeling (Spanish Fork: Banta Book Group, 2004), 139.

One of the world's largest consumers, the United States Department of Defense, followed shortly behind Wal-Mart in mandating that all of its 40,000 suppliers also implement RFID technology to help track supplies and increase efficiency. Naturally, other major companies in the civilian sector must compete with one another and any advantage that may lead to increased profits will be heavily sought after. Therefore, it is no surprise that other retailers, such as Target, Albertsons, Best Buy, and European companies Metro AG and Tesco, have joined the growing list of companies that are incorporating RFID technology in order to efficiently deal with the challenges of logistics in big business.[19]

B. ELECTRONIC PAYMENT

Another area of RFID technology application that is growing is the use of tags and readers to facilitate electronic payment. The basic concept is that when a consumer is ready to make a transaction, they simply place their tag near the reader. The tag then provides the reader with the customer's identification information; in turn, the reader sends that to a database, which associates the information to the individual's account. Finally, the purchaser's amount will be deducted from his account, all of which takes place in an instant. This application of RFID has already been used in large-scale initiatives, such as Speedpass and EZ-Pass.

[19] Patrick Sweeny, RFID for Dummies (Hoboken: Wiley Publishing, Inc., 2005), 17.

Figure 7. Speedpass tag. (From: RFI Sourcebook, p. 81)

Speedpass was created in 1997 by Mobil Oil Corporation and has grown to more than 6 million users and more than 8,900 locations in the United States alone. The idea is that a consumer can pull up to an Exxon or Mobil gas station, get fuel or other items from the adjoining convenient stores, and then wave a small wand equipped with a RFID chip next to a reader located at the gas pump or the register inside. This process simplifies the business transaction, avoiding a lengthy payment process and any potentially long lines.[20]

EZ-Pass is one of the many companies that have facilitated the application of electronic toll collection. With EZ-Pass, a car is affixed with a tag, usually on the windshield, and then as the tag passes by a reader at the toll station, it will be identified and accessed the appropriate fee. The fee will then be deducted from the associated prepaid account automatically.[21]

[20] Sandip Lahiri, *RFID Sourcebook*. (Upper Saddle River: IBM Press, 2006), 81.

[21] Ibid., 82.

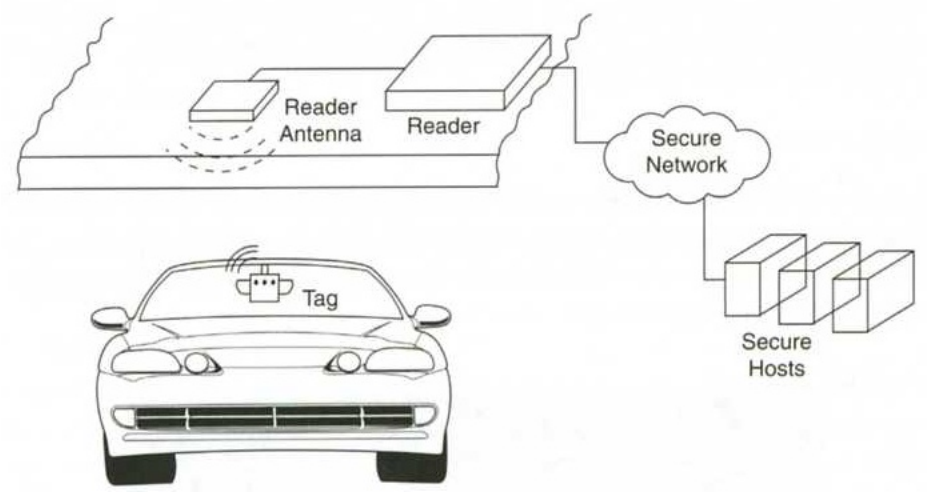

Figure 8. Electronic toll payment. (From: RFID Sourcebook, p. 82)

Whether it is avoiding lines at the register or traffic jams on the highway, the RFID application of electronic payment has proven easy and convenient. Additionally, this application eliminates the need to carry cash and proves to be more secure than many other forms of payment. Unlike debit cards, these RFID tags do not require an actual account number to be printed on the tag itself; therefore it has very little value to a potential thief. Even if someone where to steal the tag, most are limited as to the amount of money that can be prepaid into the account. It is likely that this application of RFID technology will continue to spread to most retailers and become very popular with consumers as an option of convenience.

C. ACCESS CONTROL

Access control was one of the earliest RFID applications as described in chapter II with the Los Alamos National Laboratory. It continues to be a large role for RFID today. Fort McPherson, Georgia has recently begun testing its security by employing RFID applications at the

post's gates. More than 5,000 vehicles have been registered and equipped with RFID tags in their windshields, which are compatible with the readers and database located at each of the post's entrances. When the vehicle approaches the gate its signal is received and the gate guard is then shown either an acceptance or warning light. If it is accepted, the gate will automatically open for that vehicle. If it rejected, the guard can further question the vehicle's occupant using any information that the reader might have provided as a means of further verification. For example, the database at Fort McPherson provides the guard a photo of the registered vehicle and operators, as well as expiration dates for any required certifications or inspections, which may also cause an alert if those items fall outside the requirements.[22]

D. FUTURE APPLICATIONS

While the government addresses the concerns of privacy advocates, a RFID revolution is taking place in both the U.S. government and the civilian sector. Starting in 2007, anyone applying for a U.S. passport will be issued the new e-passport, which contains a RFID tag. Tire makers will be placing RFID tags inside of their tires to assist in their safety recalls; this will begin with the commercial sector and then follow with the individual consumer. The FDA has also suggested that the makers of prescription drugs begin to implement RFID technology into their products by 2007, while the makers have gone one step further by stating that each individual bottle will eventually have a live tag on

[22] RFID Knowledgebase, "Fort McPherson Army Base, Vehicle Security" Report, IDTechEx, 18 May 2005 [Website]; Available from http://rfid.idtechex.com/knowledgebase/en/casestudy.asp?casestudyid=300; Internet; accessed 2 May 2006.

it. Citibank in New York City is creating a tag that will enable commuters to travel conveniently throughout the city's subway system. While these items have yet to come, they are not far beyond our current day applications. However, it is anticipated that tags will soon enter the home scene. The industries are already working on tags in your clothing that will inform your washing machine to use the right settings. Additionally, there will be tags on your individual food items that will let your refrigerator know what is missing inside. In turn, your refrigerator will communicate to your cell phone that you need to purchase the missing item.[23]

While we may have yet to see it, make no mistake, RFID is quickly flooding into the markets of the world and it has already begun to impact the vast majority of Americans. The question is can we apply RFID to other areas where it can affect national security on our interests abroad.

[23] Robert Tiernan, ed., "The End of Privacy," Consumer Reports, June 2006, 34-37.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RFID CONCEPTS FOR AN UNSTABLE ENVIRONMENT

In the aftermath of 9/11, Larry Ellison, the CEO of Oracle, suggested to the United States government that a national identification card be established in order to prevent any further terror attacks against the United States.[24] It was recommended that the identification card incorporate biometrics and perhaps RFID technology. However, to date nothing has materialized, as various civil liberties groups have advocated that a national ID card of any sort will infringe upon the freedoms of each and every U.S. citizen.

While the conception of a national identification card may be postponed, other existing forms of RFID embedded identification are in the works, such as the newly arriving U.S. passports, as pointed out in Chapter III. Therefore, it may just be a matter of time until this technology does enter the mainstream of American security systems and identification standards. While some Americans struggle with the implementation of RFID technology, many other nations are adopting it and benefiting from its capabilities. Despite America's resistance toward using radio frequency identification with its own citizens, perhaps the American people would be more accepting toward the use of RFID applications in other places, such as Iraq.

The purpose of this section is to describe RFID concepts that could potentially increase U.S. special operations capabilities and the security within an unstable

[24] Declan McCullagh, "The Oracle of National ID Cards," Wired News, 27 October 2001 [News online]; available from http://www.wired.com/news/conflict/0,2100,47788,00.html; Internet; accessed 21 April 2006.

environment. For reasons described in Chapter I, Iraq will be used when describing the implementation of these RFID concepts. While this section will describe the processes of each RFID component in very generic terms, it is very important to remember that the RFID community has developed a large variety of components with a diverse range of capabilities and requirements. More importantly, as each month goes by from the completion of this thesis, the technological advances that take place may render some of these recommendations outdated based on what is available to date.

A. A NATIONAL ID CARD WITH RFID TECHNOLOGY

1. The Intent of the National ID Program

The overall intent of this program is to offer instantaneous identity checks on people trafficking areas around viable targets. There are many potential benefits that could arise from the use of this technology, which will be discussed in the following chapter. However, it is important to point out now that this technology is not just a new means by which to identify insurgents, but rather this should be viewed as a force multiplier. It will provide more speed and perhaps accuracy in our identification methods and increase the number of checks we are able to conduct.

Very rarely are any countermeasures solely able to guarantee success against a threat, but when coupled with other countermeasures, they may greatly deter and render the threat ineffective. It is the intent of the national ID program to challenge the freedom of the insurgent. In order to conduct effective operations, the insurgent requires the ability to move freely. Therefore, creating a

less permissive environment for the insurgent by mandating a national ID will in essence take away his ability to conduct business as usual.

2. The Mandate

Once it has been determined that a national identification card will be utilized, a mandate must be issued to all Iraqi citizens. To ensure that all of its citizens have ample opportunity to acquire the new national identification card, a window of time should be created in which everyone must obtain the new identification card. For example, the mandate could state that all citizens of Iraq must obtain the national identification card during the month of July; anyone that has not attained this identification after July 31st is liable of non-compliance of a government mandate.

3. Emplacing the Stationary Readers

After the population has been issued the new national identification card with the embedded RFID chip, it is then time to emplace the readers. The readers should be placed in any area that is considered a high value target. For example, if an insurgent group's objective is to overthrow a government, then they will likely attempt to undermine that government's legitimacy. One way to accomplish this could be by targeting security forces, whether it is police or military, in hopes that it would show their inability to defend against the threat and possibly decrease their future capabilities. Therefore, to counter these potential attacks, readers could be positioned at all access points around police stations or military bases. Other likely targets may include airports, high traffic shopping areas, stadiums, water plants, and energy facilities, to name a few. Among other things, these stationary readers may

offer great benefits through a reduction in manpower. Ideally, multiple locations would be covered by one central monitoring station, which could conceivably be monitored by one person.

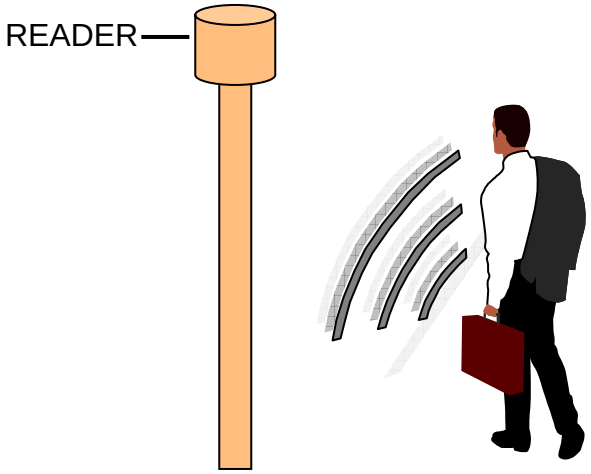

Figure 9. RFID identification card with reader.

4. The Mobile Readers

Often during times of instability, many countries will institute a program to establish random checkpoints in order to reduce the freedom of maneuver for the insurgents. These checkpoints could be established on either a roadway for vehicle access or in popular pedestrian areas, where chokepoints could be easily established with simple barriers. As mentioned in chapter II, these mobile readers require very little in terms of resources. A checkpoint could consist of just one person using a handheld reader or a fixed reader mounted on a patrolling police car.

5. The Penalty for Non-Compliance

After the cards have been issued and the readers are in place, then it is time to enact the RFID system. Basically when a person walks by a reader with his RFID

embedded identification card, then the reader will receive the signal and recognize the person's identity. At that point, either the person will be allowed to pass, or a signal will be sent out to the authorities if the person is on a watch list. However, if a person walks by a reader and no signal is received, then the reader will also send out a signal notifying the authorities that a person has passed by without identification. The ability to detect those without identification cards can be made possible with a combination of motion detectors and video surveillance. In the event that a citizen is in violation of the mandate, he will be detained immediately. Initially, an interrogation should take place on the detained citizen in order to seek an explanation of his non-compliance. If it is found that the individual had a justifiable reason for not obtaining a national ID and he is not in violation of any other laws, then he should be issued the identification card and immediately released. However, if it is determined that he intentionally avoided the issuance of the national identification card, then he should be further detained as a penalty. Potentially, some citizens might not want to adhere to the mandate, possibly for reasons of previous criminal activity or terror related activity. Clearly those falling into that category would remain in detention and then processed through the criminal justice system. While there may never be complete adherence to the mandate, it is most likely that an overwhelming majority would comply in order to carry on their livelihood and avoid potential imprisonment. On the other hand, those that oppose it, potentially insurgents, would be forced underground in order to avoid detection and carry on without government intervention.

B. RFID EMBEDDED VEHICLE IDENTIFICATION TAGS

Placing Radio Frequency Identification tags on vehicles is by no means a new idea, as pointed out in chapter III by the multiple applications of RFID already in use. In fact, the system which is described in this section nearly mirrors a system currently being tested in the United Kingdom.[25]

1. The Intent of the Vehicle Identification Tags

The intent of the RFID embedded vehicle tags is to deter insurgent movement and degrade their ability to use vehicles as weapons. This technology will enable military and law enforcement officials to instantaneously discover to whom the vehicle is registered. Clearly, if the owner is on a watch list of any sort, he can be detained at that time and his car impounded. However, it might be wiser to assume that most insurgents will not risk getting their vehicles registered for fear of getting caught at the time of registration. While this avoidance may seem an easy way out for the insurgent, it is actually still beneficial to the imposing government; it would either keep the insurgent's vehicles out of operation or force them to take a chance in driving without the proper identification tags, with a high risk of apprehension.

2. The Mandate and the Enforcement

Similar to the mandate for the national identification card, a deadline should be determined by which every Iraqi citizen should be required to register their vehicle and have the new vehicle identification tag properly displayed on their vehicle.

---

[25] Identec Solutions, "RFID-enabled License Plates to Identify UK Vehicles," RFID News, 10 June 2004 [News online] available from http://rfidnews.org/news/ 2004/06/10.rfidenabled-license-plates-to-identify-uk-vehicles/; Internet; accessed 5 April 2006.

After that deadline has passed, a strict enforcement of the mandate must follow. Vehicles that are not registered should be immediately impounded. If it is concluded that the owner was justifiably unable to get the vehicle registered, then he should be given the opportunity to register it on the spot and be released. However, if it is determined that the owner was a member of an insurgent group or that his vehicle was scheduled to be used in an upcoming attack, then the person would be held for trial and the vehicle impounded or destroyed.

3. The Vehicle Gates

In time, it is possible that every roadway and intersection could be fixed with a stationary reader. However, for this concept, it will be treated as though the number of readers is limited. Therefore, the most likely targets must be determined as was recommended in the previous section. The significant difference this time is not placing the readers immediately adjacent to the likely targets, but rather creating a substantial buffer. This must be done to potentially counter the increased threat of a vehicle in comparison to a single person, as discussed in the previous section. In other words, a vehicle can hold a much greater amount of explosives and therefore may not require being placed in the target area like a person. A vehicle could be placed adjacent to the target area, such as the case in the Oklahoma City bombing of 1995; therefore it is critical that the readers are placed far enough away from the likely targets to prevent potential damage and give military or police forces the adequate time to respond to a threat. Another key aspect in the placement of the stationary readers is placing them in a pattern which will enable those monitoring the system the ability to determine

the direction of travel of the suspected insurgent vehicle. This can be easily accomplished in two ways, by tracking the hits from multiple readers or supplementing the readers with a video monitoring system.

Figure 10. RFID vehicle tag with reader.

4. The Mobile Reader

As noted in the national identification card recommendation, it is common that an unstable country would set up random checkpoints in hopes to deter insurgent movement. Naturally, these checkpoints would be interested in vehicular identification as well as personal identification. Similar to the stationary readers, the placement of these random checkpoints should also take standoff from the potential targets into consideration. Unlike the stationary reader, the mobile reader may require at least one man to operate, unless the risk was taken to leave a mobile reader unattended. If in fact a mobile reader was being operated by someone, then additional safety measures would have to be implemented. Unlike the personnel checkpoint, vehicles provide many options to

conceal weapons or explosives that may be of harm to the reader's operator. In a worse case scenario, it could be assumed that an insurgent might use these instruments of harm once the operator learned the identity of the vehicle. As a result to counter the potential harm that the insurgent may inflict, it might be necessary to create a mobile protective barrier from which the operator can still perform his task. Additionally, it might be advantageous to provide the operator with additional armed personnel to watch over his position.

5. Conclusion

While at first glance each of these recommendations may seem to have weaknesses, it is important to understand that the idea is to run these two applications simultaneously and in coordination with one another. Naturally one might assume that with respect to the vehicle identification tag recommendation, the insurgent could just bypass the issue by stealing another person's vehicle. This in essence could work if the RFID embedded tags were an independent program, but if it is intertwined with the RFID embedded national identification card, it will be less likely to work. For example, when a vehicle passes a reader, it will receive the signal from the vehicle and at the same time it will also receive a signal from the occupant's national identification cards. If these two signals match, then the vehicle may simply proceed, but if the reader detects any discrepancies, then an alarm will be triggered. This example demonstrates the fundamental necessity of having both these initiatives working in conjunction with one another and the potential results they may provide against the insurgent population. Of course there are other potential downfalls that the insurgent will

try to take advantage of, but the overall benefits may greatly outweigh the weaknesses. The next chapter will examine the benefits and weaknesses of the RFID initiatives.

V. ADVANTAGES AND DISADVANTAGES OF RFID TECHNOLOGIES

The United States has struggled in its rebuilding efforts in Iraq and Afghanistan and it has been forced to evolve in how it contends with its enemies. The enemy has adapted to face the conventional successes of the United States Armed Forces. They have done so by exploiting areas with which we are unequipped to fight back, such as improvised explosive devices, suicide car bombs, and kidnappings. For the most part, the United States was unprepared to deal with these sorts of issues. While some gains have been made, not enough has been done. The United States must explore the advantages of upcoming technologies and determine whether or not these can help us in the Global War on Terror. It is the intent of this chapter to examine both the advantages and disadvantages of Radio Frequency Identification.

A. ADVANTAGES

1. Security

The United States Armed Forces along with the Iraqi population have endured great human losses since the liberation of Iraq from Sadam Hussein. More than 2100 U.S. service men and women have been killed as a result of hostile fire since March 2003 and Iraqi civilian casualties totaled more than 9600 for the year of 2005.[26] One of the largest contributing factors to these deaths is attacks involving the use of a vehicle by the insurgents to inflict casualties upon the Iraqi and U.S. populations. These attacks include car bombings, suicide car bombings, and use of a vehicle to run down its victims. To date the United

[26] White, Iraqi Casualties.

States and Iraqi governments have been unable to effectively combat these attacks involving vehicles. Consequently, there is no sense of security in Iraq today. In fact, recent polls have shown that the Iraqi people view the security in Iraq to be on the decline.

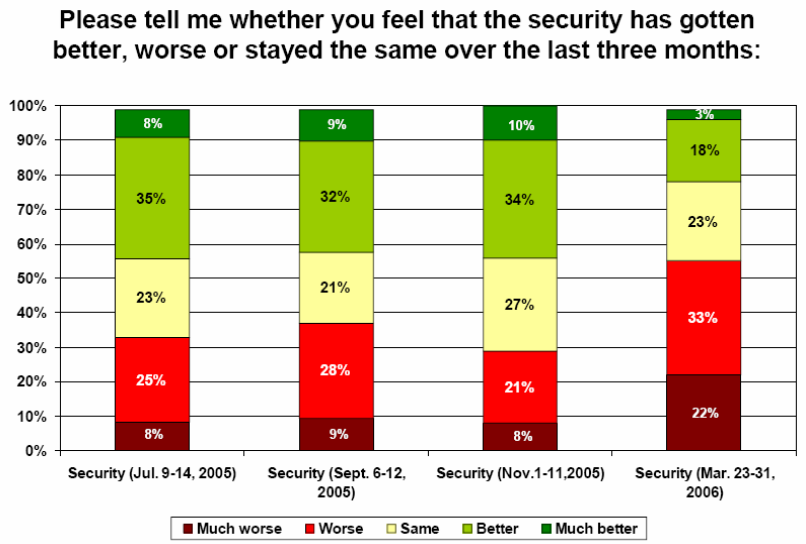

Table 1. Iraqi population poll from March 23-31, 2006. (From: Measuring Stability and Security in Iraq, p. 42)

If Radio Frequency Identification proves to be effective in deterring and preventing car related attacks or helps in the apprehension of known insurgents, it may increase the security in Iraq. This is perhaps the greatest advantage that RFID can create and it is the antithesis of what the insurgent hopes to accomplish. If the government can not provide a secure environment for its citizens, then the people may lose faith in them. This may cause the citizens to convert their trust toward the insurgents, who may appear to have control of the situation.

2. Crime Solving

Security is certainly affected by that which we can deter and prevent, but it can also be increased by solving

crimes after they have taken place and holding those responsible accountable for their acts. This is one other area where RFID can play a large role. Even in the aftermath of an attack, the RFID signals that were collected prior to the event can provide us clues about the incident and enable us to identify the perpetrators much quicker than using conventional means. Assuming that RFID readers are effective in stopping movement of personnel without the national identification cards and unregistered vehicles, we can conclude that a vehicle and its driver reaching a high value target would have had to obtain both a proper identification card and vehicle tag. While these initiatives may have failed in identifying a potential attacker, they would have recorded the identity information about the vehicle and the driver prior to the attack. Rather than having to sift through the aftermath of the car bomb to find clues, investigators can simply retrieve the data recorded by all the readers leading into the area of the attack. This potentially large list of vehicles and occupants can be quickly narrowed down by canceling out all those vehicles and drivers that registered a second outgoing signal when leaving the target area. This action alone would reduce the list of potential suspects down to those individuals and their vehicles that are still in the target area. If the attack was not a suicide bomb and the perpetrator attempted to flea the area after the attack, an alarm would be triggered as the individual passes by a reader without the corresponding vehicle he entered the area with. If any attack occurs, either law enforcement or military personnel should immediately position themselves outside of the surrounding readers, enabling them to apprehend the suspect once he has triggered the reader to

report an inconsistency. In time all of the vehicles within the area of attack will be cleared by either having passed back through a reader or being positively identified within the area of attack by investigating officials. Using this technique the end result will be the undisputable identity of the vehicle and its driver.

This process could certainly be made more rapid if a controlled evacuation of the area were to take place as officials filter each vehicle and person within the attack area out of the vicinity and past a reader. In theory, this process could take place very quickly. If the identities of the vehicle and driver were obtained, then the driver, if captured alive, could be detained and further questioned. However, if he were killed due to the attack, investigators still have the identity with which they can begin an immediate investigation.

This is a huge advantage over conventional investigative techniques, which would require much lengthier methods in identification even if the body were not disfigured from the attack. However, with the perpetrator’s signal having been recorded by a reader, an investigator can immediately look at the national database and determine the suspect’s home address and relations. With this information at hand, authorities can immediately begin a search at the perpetrator’s residence and begin questioning his family and friends. This investigative work may lead to other helpful information, such as his associates and suppliers, and potentially help unravel some of the mysteries of the terror network.

3. Economic Gain

If Radio Frequency Identification can bring a greater sense of security to an unstable environment, then economic growth may follow. Basilan, a small island in the southern province of the Philippines, was plagued by a terrorist organization known as the Abu Sayyaf Group (ASG). For years the ASG terrorized the inhabitants by committing many heinous acts, such as murder, kidnapping, extortion, and bombings. These actions were also aimed at businesses to undermine the potential economic growth on the island and in effect make the government look incompetent. These acts were very effective at forcing businesses to close and keeping outside investors away from the island. However, when U.S. military intervention took place in 2002, the Abu Sayyaf Group quickly found itself on the run and losing their control over the island's population. As time went on, many members of the organization were either captured or killed, and most of the remaining members sought refuge in other areas off the island. As a result, the feeling of security greatly increased and the island's inhabitants felt free to carry on their once regular routines. Additionally, businesses reopened and outside investors sought new opportunities as they brought the island's first franchise restaurant, Jolly Bee. The potential for economic growth was unleashed as a result of increased security. This correlation between security and economic growth is by no means unique in Basilan; it is common practice for big businesses to look for areas with stability to ensure their own long term success.

4. Less Intrusive and Time Consuming

Security check points in any setting can bring about negative feelings for those who are subject to them. Check

points may consume any sense of freedom a person could have; of course that feeling would be even greater if those manning the checkpoints are personnel from an occupying force rather than members of the host nation. Additionally, they also cause a great inconvenience for people in terms of time. Pedestrian check points can be equally as inconvenient and are reminiscent of the secret police of the former East Germany, the Stasi, or the French in Algiers. Recent polls taken in Iraq have indicated that 65% of the citizens are opposed to the presence of American forces.[27] Clearly, the eventual withdrawal of American forces will satisfy many citizens in Iraq, but reality is that it will probably take a long period of time. Therefore, in the meantime, the United States should take every measure possible to reduce the signature of U.S. forces. Additionally, it should be the aim of the Iraqi forces to do the same in due time. While it is probably unlikely that a value can be placed on the citizen's satisfaction, it is likely that lessening the physical presence of troops or police, while maintaining security could be well received. In this particular aspect, radio frequency identification has a great amount of potential toward improving public opinion. RFID applications can help reduce the physical signature of military and police presence throughout any given environment. One stationary reader could potentially replace a conventional five-person check point and still provide the same security. Additionally, the RFID portals, either permanent or mobile, will enable both pedestrian and vehicular traffic to flow

[27] Anonymous, "What Do the Iraqis Really Want," Time, 19 December 2005 [magazine online]; available from http://libproxy.nps.navy.mil/login?url=http://proquest.umi.com/pqdweb?did=942822331&sid=1&Fmt=3&clientId=11969&RQT=309&VName=PQD; Internet; accessed 16 May 2006.

at full capacity. This reduction in physical signature and time consumption will modify the current security apparatus into a less intrusive mechanism, which in turn may lessen the tensions that exist today.

5. Possible Reduction in Casualties

As stated in the last section, converting the current conventional security check points into RFID enhanced check point will greatly reduce the personnel requirements. As a result this will not only decrease the physical presence at these sites, but it will also reduce the number of potential targets for an insurgent. Attacks upon check points are not uncommon in Iraq today, but if we were to significantly reduce the numbers of personnel on these sites, we could potentially save more lives while still accomplishing the same results of the conventional check points.

Another problem today is that the personnel manning check points must remain at a high level of alertness throughout their time at the checkpoint. Currently, there is no way to distinguish between a well-intentioned citizen and an insurgent that is preparing to conduct an attack. Therefore, personnel at these check points must treat every person as a potential insurgent that is willing to take his life at any given moment. For this fact alone, it needless to say that the job related stress is extremely high. As a result, the people manning the checkpoints may be more prone to take offensive action if they feel as though their lives are threatened. Unfortunately, this may result in the deaths of innocent personnel, as was the case in Baghdad in March of 2005, when an Italian intelligence officer was killed and an Italian journalist was wounded

after violating U.S. checkpoints procedures.[28] In circumstances such as this, a RFID reader would eliminate the need for approaching vehicles to comply with any procedures, for they need only to drive past the reader. More importantly, the RFID reader will eliminate the need for personnel to distinguish between a suspect insurgent and a law-abiding citizen. Instead, the reader will identify the suspect vehicle and alert officials further down the road of the suspicious vehicle and driver. At this point, law enforcement or military personnel have gained the advantage of knowing the identity of the suspect and his vehicle and can react to them accordingly. Additionally, those officials can choose their location of apprehension of the suspect, potentially minimizing any chances of collateral damage.

6. Relatively Low-Cost

As with any new system of this magnitude, the startup cost could be high, but the cost to maintain the system would be significantly less. Without actually going through the acquisition process, a highly accurate estimate is virtually unattainable, but to better understand the relative cost, I have roughly estimated the cost to implement the two RFID applications using approximate costs given by various sources. Assuming that both the national identification cards and the vehicle identification tags can use the same readers, I have calculated an estimated cost for 10,000 fixed readers at a price of $1,500 each and 1,000 handheld readers at the high end cost of $3,000

[28] Annia Ciezadlo, "What Iraq's Checkpoints are Like," Christian Science Monitor, 7 March 2005, [newspaper online]; available from http://www.csmonitorservices.com/csmonitor/display.jhtml;jsessionid=GFYLGQMKVOYPPKGL4L2SFEQ?_requestid=83778; Internet; accessed 5 March 2006.

each.[29] For national identification cards, I have rounded up the current population of Iraq to 28 million people and estimated the price of each card to $50, the high end cost of an active tag today.[30] In regards to the vehicle identification tags, I have used a figure of 20 million vehicles and estimated the price of $100 per vehicle tag. The infrastructure buildup, establishment of a database and maintenance cost are the most difficult to determine, but for this process I have estimated one billion dollars for the first five years of expenses.

	unit price	units needed	total cost
Fixed Reader	$1,500	10000	$ 15,000,000
Handheld Reader	$3,000	1000	$ 3,000,000
National ID Cards	$50	28,000,000	$ 1,400,000,000
Vehicle Tags	$100	20,000,000	$ 2,000,000,000
Start-up/Maintenance	$1,000,000,000	1	$ 1,000,000,000
		Total =	**$ 4,418,000,000**

Table 2. An estimated cost for both RFID applications.

While these costs are staggering at first glance, these figures must be compared to the current cost of the war in Iraq today. From the beginning of the war in Iraq until September 2005, more than 197 billion dollars have been appropriated to cover the war, which is an average of 79 billion a year.[31] While the estimated five-year cost is significantly less than the current annual budget, it is still a hefty price to pay for uncertain results. Therefore, a trial basis may be better suited for implementation in Iraq. For example, these applications could be exclusively instituted in the three most violent

[29] Adrian Hawley, "RE: E-plates" Email to author, 11 April 2006.

[30] "RFID System Components and Costs," 1.

[31] Andrew Krepinevich, "The War in Iraq," (Washington, D.C: Center for Strategic and Budgetary Assessments,2005), 103.

provinces in Iraq. Then after a one-year trial, the results could be examined, and the decision to expand or stop the RFID programs could be made.

7. Operations, Maintenance, and Training

While the manufacturing and initial setup of each component must be handled by private contractors, the operational and maintenance aspects will require much less specialized attention. It is quite reasonable to assume that any soldier could operate a handheld reader with relatively little training, similar to that of a grocery store employee conducting an inventory with a conventional handheld scanner. Basically the reader itself will automatically acquire the signal from the tag. All that is required of the operator is to read the monitor and make an assessment from the information given by the database.

8. Instantaneous Tracking

While the intention of this paper is to remain neutral in aspects of individual privacy, it is important to point out all of the potential uses of Radio Frequency Identification. In the event that an individual was put on a terrorist watch list, the government could easily use the existing RFID system to monitor the individual’s movement. While this could be of great use to both military and law enforcement officials, this is also one of the major points of contention with opponents to RFID technology, as described in the later portion of this chapter.

9. Coupling RFID with Other Technologies

While RFID by itself may prove to be an effective tool in deterring insurgent activity, its potential may be even greater when matched with other technologies. For example, a RFID reader interrogating vehicle tags paired with a video camera could provide much more additional

information. First of all, the video captured could be used to match up the physical description of the vehicle to a vehicle photo that may have been put into a database at the time of registration. Even more beneficial would be the current identifying information, such as the number of occupants in the vehicle or any objects affixed to the vehicle that might not have previously been there. These description updates could be quickly broadcast to anyone involved in the apprehension of the vehicle and greatly increase their likelihood of success in finding the vehicle.

B. DISADVANTAGES

Throughout history, societies have established security measures, such as keys and identification cards, in order to prevent crimes from being committed. Despite these efforts to thwart crime, the criminal has been equally as persistent at developing counter measures to outwit these devices. The intent of this section is to address the potential threats against RFID technology, some of which have already been considered by the industry, and point out the areas that may still be a threat of exploitation.

1. Identity Theft

Just as ordinary identification cards are commonly stolen in order for a person to assume another's identity, what can be done to prevent the same type of occurrence with an RFID tag? Companies like Hills Numberplates Ltd., the maker of E-Plate, have already addressed this issue. E-Plate is a vehicle license tag that has an embedded RFID chip within it. If the license plate is tampered with, the chip will automatically self-destruct, thus killing the

signal it would otherwise broadcast to a RFID reader.[32] When the vehicle drives past a reader without a signal, an alarm would go off alerting officials to apprehend the vehicle. At that point, the enforcement officials could inspect the plate and make an assessment.

Unlike the vehicle tags, it may be more difficult to prevent identity theft with national identification cards because there is no need to remove a RFID tag, as it is self-contained in one highly mobile card. Therefore, there is a great likelihood that someone could obtain a functioning identification card from another person in order to circumvent existing security measures. For that reason, it is critical that information, such as a photo, be embedded within the tag's data in order to authenticate the card holder's identity. Additionally, facial recognition programs intertwined with the RFID applications could greatly enhance the probability of catching those who seek to beat the system.

2. Counterfeiting RFID

If an insurgent can't acquire an original RFID tag due to anti-theft measures, then why can't they manufacture one? That is exactly what one research team from John Hopkins University did as part of a study. A member of the team carrying a backpack, which concealed his equipment, walked past a test subject that was carrying the popular Speedpass from Exxon Mobil. As he passed by, the equipment that he was carrying was able to break the encryption and download the vital information from the Speedpass. At that point, the team drove to a Speedpass participating gas

[32] e-Plate – a World of RFID Solutions, "e-Plate Operation Overview," E-plate, 25 November 2005 [digital brochure]; available as e-Plate Operation Overview.pdf; e-mail; accessed 11 April 2006.

station and, using a computer, replicated the signal broadcasted by the original Speedpass, enabling them to charge gas to the actual holder's account.[33] With a plethora of RFID manufacturing companies and products, such as a relatively inexpensive printer which is capable of printing an RFID tag with a home computer, it would seem rather easy to produce a tag that could penetrate the system.

However, this is not the case if the RFID systems specifications are properly safeguarded. It is important to point out that the aforementioned study was conducted in 2005 on the Speedpass system which was created in 1997.[34] Notably, it took eight years to crack the code on a first generation technology that is considered by most in the industry to be primitive. There are many different aspects of each tag that would have to be precisely the same in order for it to properly communicate with a reader, such as the correct frequency and adequate range. Even if a person were able to produce a tag capable of communicating with a reader, then they would have to get it to transmit the right information. This would involve knowing valid identity codes and passwords, all of which would require inside help. Additionally, that information would have to be placed both on the tag and in the database, which would once again require help from within the confines of the RFID system. While potentially difficult to accomplish, we cannot rule out the possibility of an insurgent acquiring an insider's assistance, but as with any conventional

[33] Tiernan, 38.

[34] Garfinkel and Rosenberg, 179.

security measure, procedures along with checks and balances must be implemented in order to prevent these types of acts from taking place.

3. The Intrusion into Privacy

Tracking, one of RFID's greatest capabilities, is also perhaps one of its greatest weaknesses. In recent times an individual's right to privacy has headlined the national news in such incidences like the national wire tapping program run by the National Security Agency. Opponents to RFID technology argue that this technology has the potential to turn any society into that which was described as "Big Brother" in George Orwell's *1984*. Simply put, there is a fear amongst many citizens that those in control of RFID technologies can monitor anyone, at anytime. Mark Rasch, a former head of the computer-crime unit for the U.S. Justice Department, says that "RFID is the electronic equivalent of allowing everyone to snoop through your medicine cabinet."[35]

While it is not plausible to deny that this kind of misuse with RFID applications can occur, it necessary to remember that any form of surveillance needs to be properly managed to ensure that checks and balances, such as standard operating procedures and frequent inspections are in place to avoid such abuses. Radio frequency identification applications are no different than surveillance or wire tapping, and if left unmanaged they can and probably will be used improperly.

[35] Tiernan, 34.

VI. CONCLUSION

> The RFID train is beginning to leave the station… There is no downside to a public dialogue about these issues, but there are many dangers in waiting too long to start.[36]
>
> - U.S. Senator Patrick Leahy

While it is never too late to begin implementation of radio frequency identification applications, there are potential dangers in waiting longer. Dozens of members from the United States armed forces, foreign military, policeman, and nationals are dying on a daily basis, because of an inability to provide security in places like Iraq and Afghanistan.

Throughout history, many nations have had to deal with civil disobedience in various forms, ranging from refusal to pay taxes to today's frequent suicide bombings. While the first offense may be easier to deal with, the principles to deter both may be similar. When the British were experiencing problems with some of the Chinese population in Malaya during the 1950s, part of their solution was to issue identification cards to those they deemed as a risk to national stability.[37] Another historical example of dealing with civil disobedience was the East German government following World War II. In order to cope with any potential civil disobedience, the government formed the Stasi, a national secret police division, which kept close tabs on its citizens through

[36] Tiernan, 39.

[37] Frank Pelli, "Insurgency, Counterinsurgency, and the Marines in Vietnam," 1990 [Ohio State University online]; available from http://ehistory.osu.edu/vietnam/essays/insurgency/index.cfm; Internet; accessed 15 March 2006.

intensive surveillance.[38] Whether it involved the requirement for a national identification card or heavy observation of citizen activity, each countermeasure boiled down to accountability through a means of inventory. From this perspective we can compare a government providing security for its citizens to a store manager that sells a perishable product. In order to run a successful business, a manager must maintain an accurate inventory of its products and keep a careful watch on the expiration dates of those items. Both of these aspects are vital to the success of the business. If the store manager fails to keep an accurate count of his product, he runs the risk of running out of that product and having nothing to offer the consumer. Likewise, if the manager overlooks the expiration dates on his products, he may be forced to discard his inventory and forfeit his profit. Failure to conduct inventories or maintain a careful watch over a perishable product can result in a business failure. In order to understand this comparison we can substitute the store manager with a nation's government, and the product with the citizens of that nation. In this situation the government must also keep an inventory of its citizens through various methods such as a census, a national database, a national identification card, or perhaps a combination of these. A nation's failure to maintain accountability of its citizens could result in the inability to provide for them and the possibility of being unable to determine the identity of those who are a risk to that nation's security. Similar to the previous example, a government must also keep watch on its citizens, for they too can go bad like a perishable item. If left unchecked,

[38] John Koehler, Stasi (Boulder: Westview Press, 1999), 9.

a citizen or a group of citizens can develop a movement with the intent to threaten a nation's security or undermine the government itself. Maintaining the same point of reference, can we use RFID to help assist a foreign nation or the U.S. armed forces in maintaining security through an inventory-minded approach? If one can conceptualize the inventory approach, it is an easy step to understanding how RFID technology can provide an advantage to those trying to maintain order. As pointed out in Chapter III, RFID has revolutionized the business world by increasing overall efficiency and reducing human intervention. These same benefits could be applied to areas of instability by providing our armed forces valuable real-time information about the public at large. Instituting the RFID applications recommended in Chapter IV could produce the same positive results for the Department of Defense, which RFID has delivered in the civilian business sector.

Despite the numerous advantages that these RFID concepts could provide, the greatest challenge might be convincing the populations where these are to be implemented that there are great benefits to be gained in exchange for minor modifications in their daily lives. Similar initiatives, such as the Real ID Act and RFID embedded passports, have faced large opposition in the United States and continue to face the threat of being brought to a halt. Certainly some will protest that RFID will impose upon their personal freedoms, but in actuality, it would not if it is responsibly managed. Some resistance to RFID technology is good, in that it requires manufacturers to incorporate the opponent's concerns into

their applications and alerts governments to potential weaknesses in RFID products. While citizens may be monitored more than before, they can continue to conduct themselves in the same manner that they have been. Only those that partake in illegal and potentially harmful acts should pay a price as law enforcement may gain the upper hand through the increased technology. However, the potential benefits of increased national security may greatly outweigh any negative aspects associated with the RFID concepts recommended within this thesis. Australia, Malaysia, Mexico, South Africa, Sri Lanka, Sweden, the United States, and the United Kingdom, amongst others, are already implementing similar RFID related security measures, and it is potentially a short matter of time before this technology revolutionizes the world of security.[39]

[39] Lahiri, 84-87.

LIST OF REFERENCES

"Glossary of RFID Terms," RFID Journal [journal online]; available from http://www.rfidjournal.com /article/articleview/1338/1/129; Internet; accessed 21 April 2006.

"Introduction to RFID," Identec Solutions. Available from http://www.identecsolutions.com/ intro_to_rfid.asp; Internet; accessed 3 May 2006.

"RFID System Components and Costs," RFID Journal [journal online]; available from http://www.rfidjournal.com /article/articleview/1338/1/129; Internet; accessed 21 April 2006.

"The History of RFID Technology," RFID Journal [journal online]; available from http://www.rfidjournal.com /article/articleview/1338/1/129; Internet; accessed 21 April 2006.

Albrecht, Katherine, and Liz McIntyre. *Spychips*. Nashville: Nelson Current, 2005.

Anonymous, "What Do the Iraqis Really Want," Time, 19 December 2005 [magazine online]; available from http://libproxy.nps.navy.mil/login?url=http://proquest .umi.com/pqdweb?did=942822331&sid=1&Fmt=3&clientId=119 69&RQT=309&VName=PQD; Internet; accessed 16 May 2006.

Bandow, Doug, James Bovard, Richard Ebeling, Jacob Hornberger, and Sheldon Richman. Liberty, Security, and the War on Terrorism. Fairfax: The Future of Freedom Foundation, 2003.

Bayley, David. *Forces of Order: Police Behavior in Japan and the United States*. Berkley: University of California Press, 1976.

Childs, David. *The Stasi: The East German Intelligence and Security Service*. New York: New York University Press, 1996.

Ciezadlo, Annia. “What Iraq’s Checkpoints are Like,” Christian Science Monitor, 7 March 2005, [newspaper online]; available from http://www.csmonitorservices.com/csmonitor/display.jhtml;jsessionid=GFYLGQMKVOYPPKGL4L2SFEQ?_requestid=83778; Internet; accessed 5 March 2006.

Currer-Briggs, Noel, ed. *Security: Attitudes and Techniques for Management*. London: Hutchinson & Co., 1968.

Department of Defense. “Daily Casualty Report.” 1 June 2006. Website. Available from http://www.defenselink.mil/news/casualty.pdf; Internet; accessed 1 June 2006

e-Plate – a World of RFID Solutions, “e-Plate Operation Overview,” E-plate, 25 November 2005 [digital brochure]; available as e-Plate Operation Overview.pdf; e-mail; accessed 11 April 2006.

Field, Stewart, and Caroline Pelser, eds. *Invading the Private: State Accountability and New Investigative Methods in Europe*. Brookfield: Ashgate Publishing Company, 1998.

Flynn, Stephen. *America the Vulnerable: How Our Government is Failing to Protect Us from Terrorism*. New York: Harper Collins Publishers Inc., 2004.

Garfinkel, Simson, and Beth Rosenberg, eds. *RFID: Applications, Security, and Privacy*. Upper Saddle River: Addison Wesley, 2006.

Hawley, Adrian. “RE: E-plates.” Email to author, 11 April 2006.

Heyman, Philip. *Terrorism, Freedom, and Security: Winning without War*. Cambridge: The MIT Press, 2003.

Identec Solutions. “RFID-enabled license Plates to Identify UK Vehicles.” RFID News, 10 June 2004. News online. Available from http://rfidnews.org/news/2004/06/10.rfidenabled-license-plates-to-identify-uk-vehicles/; Internet; accessed 5 April 2006.

Kleist, Robert, Theodore Chapman, David Sakai, and Brad Jarvis. *RFID Labeling*. Spanish Fork: Banta Book Group, 2004.

Koehler, John. *Stasi*. Boulder: Westview Press, 1999.

Krepinevich, Andrew. "The War in Iraq: An Interim Assessment." Washington, D.C: Center for Strategic and Budgetary Assessments, 2005.

Lahiri, Sandip. *RFID Sourcebook*. Upper Saddle River: IBM Press, 2006.

Landt, Jeremy. "Shrouds of Time: The History of RFID", AIM {whitepaper online]; available from http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf; Internet; accessed 26 April 2006.

Leites, Nathan and Charles Wolf. *Rebellion and Authority: An Analytic Essay on Insurgent Conflicts*. Chicago: Markham Publishing Company, 1970.

Libiki, Martin. "Are RFIDs Coming to Get You?" IEEE Security & Privacy, Vol. 3, Num. 6 (2005): 6.

Mahajan, Rahul. *The New Crusade: America's War on Terrorism*. New York: Monthly Review Press, 2002.

McCullagh, Declan. "The Oracle of National ID Cards." Wired News, 27 October 2001. News online. Available from http://www.wired.com/news/conflict/0,2100,47788,00.html; Internet; accessed 21 April 2006.

National Security Strategy (Washington, D.C: 2006), Preface.

O'Hanlon, Michael, Peter Orszag, Ivo Daalader, I. Destler, David Gunter, James Lindsay, Robert Litan, and James Steinberg. *Protecting the American Homeland: One Year On*. Washington, D.C.: Brooking Institution Press, 2002.

Pelli, Frank. "Insurgency, Counterinsurgency, and the Marines in Vietnam." Global Security, 1990. Report online; Available from http://www.globalsecurity.org/military/library/report/1990/PFD.htm; Internet; accessed 8 June 2006.

Phillips, Ted, Tom Karygiannis, and Rick Kuhn. "Security Standards for the RFID Market." IEEE Security & Privacy, Vol. 3, Num. 6 (2005): 85-89.

Reuters, “U.S. Retired Generals Debate over Rumsfeld,” MSNBC 16 April 2006 [website]; available from http://www.msnbc.msn.com/ default.aspx?id=9974867; accessed 21 April 2006.

RFID Knowledgebase. “Fort McPherson Army Base, Vehicle Security” Report, IDTechEx, 18 May 2005. Website. Available from http://rfid.idtechex.com/ knowledgebase/en/casestudy.asp?casestudyid=300; Internet; accessed 2 May 2006.

Shepard, Steven. *RFID: Radio Frequency Identification*. New York: McGraw Hill, 2005.

Sweeny, Patrick. *RFID for Dummies*. Hoboken: Wiley Publishing, Inc., 2005.

Tiernan, Robert, ed. “The End of Privacy.” Consumer Reports, June 2006.

U.S. Government. “Measuring Stability and Security in Iraq.” Report to Congress, 30 May 2006. Report Online. Available from http://www.defenselink.mil/home/ features/Iraq_Reports/Index.html; Internet; accessed 2 June 2006.

White, Jonathan. *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security*. Toronto: Wadsworth/Thompson, 2004.

White, Michael. “Iraq Coalition Casualty Count,” *Icasualties*, 1 June 2006 [homepage]; available from http://www.icasualties.org/oif/ default.aspx; Internet; accessed on 1 June 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California